CLAIMS:

1. A method of handling data packets in a network device, said method comprising:

receiving an incoming data packet;

parsing the incoming data packet to obtain a portion of the incoming data packet;

comparing said portion with rules stored in a rule table, where each rule of said rules specifies a set of actions;

selecting a match between said portion and a particular rule of said rules; and

executing a particular set of actions specified by said particular rule;

wherein each rule field of said rules includes a mask and a selection flag used in the comparing said portion with each rule.

2. A method of handling data packets as recited in claim 1, wherein the step of comparing said portion with rules stored in a rule table comprises comparing specific fields of the incoming data packet with corresponding rule fields in all of the rules stored in the rule table.

3. A method of handling data packets as recited in claim 2, wherein specific fields of the packet include a source port identification number and layer 2 to layer 7 headers.

4. A method of handling data packets as recited in claim 1, wherein the step of selecting a match between said portion and a particular rule of said rules

comprises selecting a highest priority rule of said rules to be the particular rule when more than one rule of said rules match said portion.

5. A method of handling data packets as recited in claim 4, wherein the highest priority rule is determined by the addresses of said rules within said rules table.

6. A method of handling data packets as recited in claim 1, wherein said mask comprises an encoded compact mask and the step of comparing said portion with rules stored in a rule table comprises:

applying said encoded compact mask of said rule fields to corresponding fields of the incoming data packet to obtain a packet field value;

comparing the packet field value with a rule field value contained in said one of said rules; and

examining the selection flag of said one of said rule fields to determine whether said one of said rules is a potential match.

7. A method of handling data packets as recited in claim 6, wherein each rule has at least three types of rule fields comprising:

rule fields with a fixed location and a compact mask,

rule fields with a fixed field location and a full mask that is as wide as the packet field value, and

rule fields with a programmable field location which allows the rule field value to be mapped to any contiguous section of said portion of the incoming data packet.

8. A method of handling data packets as recited in claim 6, wherein the step of applying said mask of one of the rules comprises expanding the compact mask to a full mask as wide as the packet field value and applying the full mask to said portion.

9. A method of handling data packets as recited in claim 8, wherein the full mask is applied to said portion to obtain at least one of an IP destination address and an IP source address as the packet field value.

10. A method of handling data packets as recited in claim 7, further comprising the step of examining a global programmable flag to determine whether a start address of the programmable field location is a beginning of a layer 2 header or a layer 3 header of the incoming data packet.

11. A method of handling data packets as recited in claim 6, wherein the step of examining the selection flag comprises inverting the result of the comparing the packet field value step when the selection flag is set to a particular value.

12. A method of handling data packets as recited in claim 6, wherein the method further comprises determining a validity of the packet field value and using the determination to decide whether said one of said rules is the potential match.

13. A method of handling data packets as recited in claim 12, wherein the step of determining a validity of the packet field value comprises parsing said portion of the data packet to determine the validity and returning the validity result and the

packet field value.

14. A method of handling data packets as recited in claim 12, wherein the step of determining a validity of the packet field value comprises comparing one or more programmable rule fields with certain packet field values in the incoming data packet, and, when the one or more programmable rule fields do not match, overriding comparison results of all other rule fields in the same rule.

15. A method of handling data packets as recited in claim 14, wherein the step of comparing one or more programmable rule fields with certain packet field values comprises determining how many bytes of the packet field value of the incoming data packet are present and indicating the rule field is not the match when mask bits of invalid bytes of the rule field value are not set to zeros.

16. A method of handling data packets as recited in claim 13, wherein the step of parsing said portion to determine validity further comprises determining whether a particular section of said portion required for a selected rule field value is present in the parsed portion.

17. A method of handling data packets as recited in claim 12, wherein the step of determining a validity of the packet field value comprises determining that one of said rules is the potential match when the packet field value is invalid but the compact mask of the rule field is all zeros.

18. A method of handling data packets as recited in claim 12, wherein the step of determining a validity of the packet field value comprises determining that one of said rules is the potential match when the packet field value is invalid but a valid bit of the rule field is set to zero.

19. A method of handling data packets as recited in claim 1, wherein the step of executing a particular set of actions specified by said particular rule comprises modifying a header of the incoming data packet, forwarding the incoming data packet to a destination address, or updating a management information register.

20. A method of handling data packets as recited in claim 19, wherein the step of updating a management information register comprises providing a bitmap used to increment individual counters indicating a forwarding, dropping, or processing of certain types of packets.

21. A method of handling data packets as recited in claim 19, wherein said particular set of actions comprises setting a flow identification for the incoming data packet such that the packet is classified according to a class of service.

22. A method of handling data packets as recited in claim 1, wherein the step of comparing said portion with rules stored in a rule table comprises comparing said portion with rules stored in a rule table implemented in a static random access memory, with three types of rule fields and action fields all stored in each row of the static random access memory.

23. A method of handling data packets as recited in claim 1, wherein the step of comparing said portion with rules stored in a rule table comprises comparing said portion with rules stored in a rule table implemented in a content addressed memory, where each entry of the content addressed memory includes a selection flag and a validity bit.

24. A network device for handling data packets comprising:

a rules table;

means for receiving an incoming data packet;

means for parsing the incoming data packet to obtain a portion of the incoming data packet;

means for comparing said portion with rules stored in said rule table, where each rule of said rules specifies a set of actions;

means for selecting a match between said portion and a particular rule of said rules; and

means for executing a particular set of actions specified by said particular rule;

wherein each rule field of said rules includes a mask and a selection flag used by the means for comparing said portion with each rule.

25. A network device for handling data packets as recited in claim 24, wherein the means for comparing said portion with rules stored in a rule table comprises means for comparing specific fields of the incoming data packet with corresponding rule fields in all of the rules stored in the rule table.

26. A network device for handling data packets as recited in claim 25, wherein specific fields of the packet include a source port identification number and layer 2 to layer 7 headers.

27. A network device for handling data packets as recited in claim 24, wherein the means for selecting a match between said portion and a particular rule of said rules comprises means for selecting a highest priority rule of said rules to be the particular rule when more than one rule of said rules match said portion.

28. A network device for handling data packets as recited in claim 27, wherein the means for selecting a highest priority rule determines the highest priority rule by examining the addresses of said rules within said rules table.

29. A network device for handling data packets as recited in claim 24, wherein said mask comprises an encoded compact mask and the means for comparing said portion with rules stored in a rule table comprises:

means for applying said encoded compact mask of said rule fields to corresponding fields of the incoming data packet to obtain a packet field value;

means for comparing the packet field value with a rule field value contained in said one of said rules; and

means for examining the selection flag of said one of said rule fields to determine whether said one of said rules is a potential match.

30. A network device for handling data packets as recited in claim 29, wherein each rule has at least three types of rule fields comprising:

rule fields with a fixed location and a compact mask,

rule fields with a fixed field location and a full mask that is as wide as the packet field value, and

rule fields with a programmable field location which allows the rule field value to be mapped to any contiguous section of said portion of the incoming data packet.

31. A network device for handling data packets as recited in claim 29, wherein the means for applying said mask of one of the rules comprises means for expanding the compact mask to a full mask as wide as the packet field value and means for applying the full mask to said portion.

32. A network device for handling data packets as recited in claim 31, wherein the means for applying the full mask obtains at least one of an IP destination address and an IP source address as the packet field value.

33. A network device for handling data packets as recited in claim 30, further comprising means for examining a global programmable flag to determine whether a start address of the programmable field location is a beginning of a layer 2 header or a layer 3 header of the incoming data packet.

34. A network device for handling data packets as recited in claim 29, wherein the means for examining the selection flag comprises means for inverting the result of the means for comparing the packet field value, where the means for inverting inverts the result when the selection flag is set to a particular value.

35. A network device for handling data packets as recited in claim 29, wherein the network device further comprises means for determining a validity of the packet field value and decision means to decide whether said one of said rules is the potential match.

36. A network device for handling data packets as recited in claim 35, wherein the means for determining a validity of the packet field value comprises means for parsing said portion of the data packet to determine the validity and means for returning the validity result and the packet field value.

37. A network device for handling data packets as recited in claim 35, wherein the means for determining a validity of the packet field value comprises means for comparing one or more programmable rule fields with certain packet field values in the incoming data packet, and, means for overriding comparison results of all other rule fields in the same rule, where the means for overriding comparison results acts when the one or more programmable rule fields do not match,

38. A network device for handling data packets as recited in claim 37, wherein the means for comparing one or more programmable rule fields with certain packet field values comprises means for determining how many bytes of the packet field value of the incoming data packet are present and means for indicating the rule field is not the match when mask bits of invalid bytes of the rule field value are not set to zeros.

39. A network device for handling data packets as recited in claim 36,

wherein the means for parsing said portion to determine validity further comprises means for determining whether a particular section of said portion required for a selected rule field value is present in the parsed portion.

40. A network device for handling data packets as recited in claim 35, wherein the means for determining a validity of the packet field value comprises means for determining that one of said rules is the potential match when the packet field value is invalid but the compact mask of the rule field is all zeros.

41. A network device for handling data packets as recited in claim 35, wherein the means for determining a validity of the packet field value comprises means for determining that one of said rules is the potential match when the packet field value is invalid but a valid bit of the rule field is set to zero.

42. A network device for handling data packets as recited in claim 24, wherein the means for executing a particular set of actions specified by said particular rule comprises means for modifying a header of the incoming data packet, means for forwarding the incoming data packet to a destination address, or means for updating a management information register.

43. A network device for handling data packets as recited in claim 42, wherein the means for updating a management information register comprises means for providing a bitmap used to increment individual counters indicating a forwarding, dropping, or processing of certain types of packets.

44. A network device for handling data packets as recited in claim 42, wherein the means for executing a particular set of actions comprises means for setting a flow identification for the incoming data packet such that the packet is classified according to a class of service.

45. A network device for handling data packets as recited in claim 24, wherein the rule table is implemented in a static random access memory, with three types of rule fields and action fields all stored in each row of the static random access memory.

46. A network device for handling data packets as recited in claim 24, wherein the rule table is implemented in a content addressed memory, where each entry of the content addressed memory includes a selection flag and a validity bit.